STATEMENT FOR THE RECORD

ON BEHALF OF

THE NATIONAL ASSOCIATION OF CONVENIENCE STORES

AND

THE SOCIETY OF INDEPENDENT GASOLINE MARKETERS OF AMERICA

FOR THE

HEARING OF THE SENATE COMMERCE SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE AND DATA SECURITY

FEBRUARY 5, 2015

"GETTING IT RIGHT ON DATA BREACH AND NOTIFICATION LEGISLATION IN THE 114TH CONGRESS"

Chairman Moran, Ranking Member Blumenthal and members of the subcommittee, thank you for giving us the opportunity to submit this statement for the record on the topic of the elements of sound data breach legislation. We are submitting this statement on behalf of both the National Association of Convenience Stores (NACS) and the Society of Independent Gasoline Marketers of America (SIGMA).

NACS is an international trade association composed of more than 2,200 retail member companies and more than 1,600 supplier companies doing business in nearly 50 countries. The convenience and petroleum retailing industry has become a fixture in American society and a critical component of the nation's economy. In 2013, the convenience store industry generated almost $700 billion in total sales, representing approximately 2.5% of United States GDP.

SIGMA represents a diverse membership of approximately 270 independent chain retailers and marketers of motor fuel. Ninety-two percent of SIGMA's members are involved in gasoline retailing. Member retail outlets come in many forms, including travel plazas, traditional "gas stations," convenience stores with gas pumps, cardlocks, and unattended public fueling locations. Some members sell gasoline over the Internet, many are involved in fleet cards, and a few are leaders in mobile refueling.

Collectively, NACS and SIGMA represent an industry that accounts for about 80 percent of the motor fuel sales in the United States. And, this is truly an industry of small businesses. While many motor fuel outlets have agreements to use the brand names of major oil companies, those oil companies have largely exited the retail market. The vast majority of those branded outlets are locally owned. For example, more than 70 percent of the NACS' total membership is composed of companies that operate ten stores or less, and more than 60 percent of the membership operates a single store.

With this testimony, we will briefly lay out the interest our members have in data breach legislation, note how the payment card system impacts our data security efforts, provide background on data breaches, note the current state of the law on data breach notification, and walk through the elements of data breach legislation that we consider to be most important. We also note that protecting against data breaches ought to be a primary focus given that notice laws have already proliferated around the country.

Convenience and Motor Fuel Outlets Interest in Data Breach Legislation

With so many small businesses, some may wonder why our industry is concerned about data breaches. Our retailers typically do not store much information about their customers. They store employee information, but the primary reason data breaches affect these small, medium, and larger businesses is that these retailers handle payment card information in order to facilitate transactions that occur every day. In light of the number of fuel and other transactions that our industry engages in, we handle approximately one of every 22 dollars spent in the United States. In fact, our retailers serve about 160 million people per day – around half of the U.S. population. And, a majority of those transactions are made using payment cards.

The Payment Card System in the United States

Unfortunately, in the United States, payment card information is more vulnerable and enticing to data thieves than it should be. The dominant payment card networks, Visa and MasterCard, control the security of payment cards through promulgating their own proprietary specifications for those cards and their use as well as through the Payment Card Industry (PCI) organization they created and dominate. PCI not only sets data security standards for cards and card issuance, but also for retailers, like NACS and SIGMA members, that accept such cards. This creates an odd dynamic. The companies we represent, and other retailers, do not decide their own data security standards, the payment card networks do that.

Having PCI set data security standards for retailers has not worked well. PCI has consistently put the profits of the companies that control it (principally, Visa and MasterCard) before good security. They have set standards that are both more expensive for retailers than they should be and less effective at providing security than they should be. That is a remarkable combination. Unfortunately, as card security expert Avivah Litan of Gartner Research wrote recently, "The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history."[1]

For example, the cheapest, most effective way to better protect against the fraudulent use of payment card numbers is to require another piece of information with those numbers in order to make them useable. The financial industry knows this well. That is why, every time any one of us uses a payment card – whether it's a debit or a credit card – to access our accounts at an automated teller machine (ATM), we enter a personal identification number (PIN). If we don't enter a PIN, we don't get to engage in a transaction. The account number of the card is meant to demonstrate the actual card is there and being used (though this has become less effective in the last generation leading to the move to computer chips in cards throughout the world), and the PIN is meant to demonstrate that the person using the card is the person authorized to do so. It does not make sense that the same financial institutions that insist a PIN is used to authenticate the person when someone tries to enter into a transaction with them, do not want consumers to have to enter a PIN when they enter into a transaction with a merchant.

The reason that financial institutions are not as interested in protecting against fraud on transactions with merchants as they are in protecting against fraud on transactions with financial institutions themselves is that those financial institutions push many of the losses from fraudulent transactions onto merchants. While the financial industry often claims that it provides merchants with a "payment guarantee", it does no such thing. The Federal Reserve studied this a few years ago and found that, on debit transactions that did not use a PIN, merchants paid for more than 40 percent of fraud losses.[2] On credit card transactions, merchants pay for the majority of fraud losses. At our members' gas pumps, for example, we pay for about 74 percent of fraud losses on debit and credit cards.[3]

[1] "How PCI Failed Target and U.S. Consumers," by Avivah Litan, Gartner Blog Network, Jan. 20, 2014, available at http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/.
[2] 77 Fed. Reg. 46261, 46262 (Aug. 3, 2012).
[3] *Id.*

That is a major reason why PCI does not have the incentive to require the most effective security. The institutions that have the primary voice in PCI's work don't feel the full brunt of the economic consequences of their decisions.

What does this mean for the security of payment card data? Well, if payment card numbers themselves could not be monetized, there would be far less financial incentive for thieves to try to steal that information. PIN numbers are harder to steal than payment card numbers because PINs are typically encrypted as they are entered and remain that way for most of their travels through the payment card system. The major breaches that have garnered news attention during the past year – at banks and at merchants – have not involved the loss of PINs. There is some ability for data thieves to guess some PINs and, at the margins, find some ways to monetize payment card data even when PINs are required. But thieves' ability to make money from stolen payment card numbers is greatly diminished when PINs are required.

Requiring the use of PINs is not a silver bullet solution. There is far more to it than that. But, the failure of the financial industry to make that simple move, and one that is cheap and easy for the vast majority of merchants, is emblematic of the problems we all face protecting payment card data from breaches today.

The Picture of Data Breaches

Data thieves steal information from every type of organization in the United States. No one is immune. Manufacturers, utilities, services companies, health care providers, educational institutions, not-for-profits, telecommunications companies, banks, credit unions, payment card networks, payment card processors and merchants have all suffered data breaches. In fact, government agencies also suffer data breaches. Victims of breaches have even included the Defense Department and National Security Agency. These organizations are true experts in this area that go to great lengths to protect their systems. But, again, no one is immune.

Unfortunately, data thieves today include foreign countries and well-funded, sophisticated organized crime organizations, among many others. These thieves know where vulnerabilities are and relentlessly work to exploit them. It is very difficult to protect against these thefts. U.S. entities that suffer data breaches are victims of these crimes. That does not mean they shouldn't have any responsibilities when they are victimized, but it's worth remembering when some want to take a punitive approach to those who suffer breaches.

The Verizon Data Breach Investigations Report is the most comprehensive summary of data threats. The 2014 report (examining 2013 data) determined that there were 63,437 data security incidents reported by industry, educational institutions and governmental entities last year and that 1,367 of those had confirmed data losses. Of those with confirmed data losses, the financial industry suffered 34%, public institutions (including governmental entities) had 12.8%, the retail industry had 10.8%, hotels and restaurants combined had 10%, and, as noted above, other sectors suffered breaches as well. When reviewing these numbers, it is worth keeping in mind that there are approximately 1,000 times as many retailers in the country as there are financial institutions.

Current State of the Law

Before getting into questions about a potential federal data breach law, it is worth taking a look at the current state of the law. A total of 51 U.S. states and territories have data breach laws on the books today. Companies comply with these laws every day. This is not an area in which there is a lack of regulation.

Many of these 51 laws are very similar. While there may be some benefits to streamlining this system by having one federal law that pre-empts these 51 different laws, that should only be done if it can improve upon the current law. It would be simpler and cheaper for businesses to comply with one law than with many, but that is not the only value at stake in this discussion. Any effort to write federal legislation should take care not to introduce problems that the current law does not have.

Elements of Data Breach Law

There are several elements that we see as important to a federal law on data breach. First, the law should not have holes in it that result in consumers not getting notice. Second, the law should create a level playing field for businesses so that it does not introduce gaps that data thieves can exploit and does not overly burden any particular sector of the economy. Third, the law needs to have sufficient flexibility to cover the many different circumstances arising from different data breaches. This includes requiring notice only when it makes sense to do so and allowing sufficient flexibility on timing for proper investigations of data incidents to take place. Fourth, the law should not take a punitive approach to businesses that have their data stolen by thieves. Fifth, if there is going to be a law, it should pre-empt state laws. There is no need for a fifty-second data breach law.

Don't Create Notice Holes

In most instances, when data breaches happen today, consumers can have confidence that if the breach exposes data in a way that may harm them, they will get notice. The 51 different laws around the country help ensure that this happens. That is as it should be.

There are, however, exceptions to this general confidence. The data breach guidance put in place pursuant to the Gramm Leach Bliley Act (GLBA), for example, does not provide such confidence when financial institutions have data breaches. GLBA guidance says that banks and credit unions should have response plans in place in case their systems are breached, but those response plans are not actually required.[4] GLBA guidance recommends that financial institutions have plans in place to provide consumer notification of data breaches, but again those plans are not required.[5] Following a breach, GLBA guidance says that banks should conduct an

[4] Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS) at ¶ III, C.

[5] Incident Response Guidance, 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12

investigation to determine the likelihood that information has been or will be misused as a result of the breach, but that investigation is not required.[6] GLBA guidance also provides that if a financial institution determines that customer information has been or is likely to be misused then the institution should notify its customers.[7] But, here again, such notice is not required. In short, GLBA results in a system of law in which financial institutions have discretion over how closely to look at their data breaches and whether to inform their customers, if at all. In fact, we are not aware of any financial institutions that have been investigated and fined for not adequately looking into a data breach or not providing customers with notice of such a breach.

Last August, JP Morgan Chase suffered the largest data breach in U.S. history. That breach was reportedly part of a pattern of breaches of financial institutions that included breaches of perhaps a dozen or so banks. In spite of this, only a few of the names of these banks have ever been reported. In fact, even the JP Morgan Chase breach became public only because there was a reference to it in a filing the bank made with the Securities and Exchange Commission. Once it became a front page story, JP Morgan Chase provided notice of its breach. It is not clear which of the other affected banks did the same. And, under GLBA, that appears to be just fine. In October, the USA Today reported that FBI officials had warned that 500 million financial records had been stolen from banks over the previous year. It is not clear how many of those incidents resulted in notice to consumers.

Thankfully, the majority of state laws help patch this major shortcoming in federal law. Based on our analysis, thirty-seven of the fifty-one state and territorial data breach laws cover banks while fourteen of them exempt banks. That helps, but it isn't good enough to provide consumers with the confidence they should have that they will get notice when it is warranted. Any federal law on data breach needs to fix this hole in the current notice system or it is ignoring the most prominent shortcoming of the current system of notice for data breaches around the country.

Create a Level Playing Field

Ensuring there are no holes in data breach notice provisions goes hand-in-hand with establishing a level playing field for businesses that handle data. Many types of data are transmitted between different businesses on a regular basis but this is particularly true of payment card data. In fact, merchants, data line providers, processors, acquiring banks, card networks, and card issuers transmit data back-and-forth among one another hundreds of millions of times per day. If data breach legislation focuses on some of these businesses and does not cover others the same way, a couple of problems will result. One is that the lack of standards for some will, because the businesses will operate with different incentives, lead to data security gaps that thieves will exploit. Two is that some businesses will take on the brunt of the costs and reputational harms that can come with notice responsibilities even when they are not responsible for some of those breaches. That would not be appropriate.

C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS) [hereinafter *Response Guidance*].

[6] *Id.*

[7] *Id.*

The problem of data security weaknesses in the transfer of data among businesses is already part of the landscape. For example, merchants are required by the payment card companies to encrypt payment card data when they hold it on their systems. But, financial institutions are not required to be capable of accepting that data in encrypted form. The result is that data must be de-encrypted as it runs through the payment system in order to complete a transaction.[8] Data thieves have targeted these points of vulnerability in past data breaches. If we are going to have federal legislation, it should avoid creating similar gaps by covering everyone in the payment data chain with the same laws.

For some reason, telecommunications providers have argued that they should not have the same responsibilities as other companies that handle data. Some have raised a fallacious concept to justify this position. They claim that data lines controlled by telecommunications providers are "dumb pipes." Nothing could be further from the truth. Data lines include switches and routers throughout them that can monitor the carriage of data, watch for problems, and ensure transmissions get to the right place. This is all necessary to making the system operate correctly.

But these complexities are why the Federal Communications Commission and the Congress are considering the issue of net neutrality. If telecommunications lines were actually "dumb" they could not be anything other than neutral. We are not aware, for example, of anyone calling on this committee to examine water or sewer line neutrality. The phrase and concept of "dumb pipes" simply has no place in the discussion of data breaches.

The switches and routers in telecommunications lines consist of millions of lines of computer code – and they have vulnerabilities. In fact, by law these systems are required to have backdoors allowing the companies to tap those lines and access the data being sent. Those requirements are in place so that law enforcement can gather information being transmitted when appropriate. When legitimate actors can access communications in transit to monitor data, unfortunately, illegitimate ones can as well. No one's system is completely immune from data thieves. Telecommunications providers, just like other businesses, have suffered data breaches in the past. There is no principled basis for absolving these companies from the responsibilities that others have when their systems are breached.

Other businesses should not carry the burden, reputational or otherwise, when telecommunications companies suffer breaches. That is especially true of small businesses. These businesses work hard to secure their own systems, but they don't have the same resources or sophistication to follow the work of data thieves that big businesses (including many telecommunications companies) do. If a telecommunications provider or financial institution tells a small business that the small business suffered a breach, that small business usually accepts that as fact. But the initial assessment of where a breach occurred is often wrong and if the telecommunications provider and financial institution do not have their own legal responsibilities regarding breaches of their systems, many breaches will be laid at the doorstep of others and no one will ask more questions. If a federal law is going to empower regulators to look into these situations, they must have the latitude to look at everyone involved to ensure they

[8] The Nilson Report, Issue 934, Sept. 2009 at 7.

live up to their responsibilities – and don't simply pawn off those responsibilities onto smaller players with fewer resources.

Provide Flexibility

Data breaches can be difficult to detect and it can be even more difficult to determine the full extent of some of them. The complexity of breaches has consistently increased over time along with the increased sophistication and funding of organized crime. In fact, two-thirds of data breaches take months to discover.[9] Providing public notice of data breaches before the full extent of a breach is known, and therefore before a business can be sure that its system is fully secure, can create increased risk for consumers and business. If data thieves become aware that they have been detected, which notice would make clear, they often try to quickly grab as much additional data as they can as fast as they can. That is not a risk that legislation needs to create by setting an arbitrary timing requirement for notice. While many laws provide exceptions to notice requirements when law enforcement requests a delay, that alone may not be sufficient to protect against this type of problem.

In order to avoid setting a requirement that notice be given before a system is fully secured, a flexible timing requirement that includes the concept of the business need for fully protecting against further data theft would be wise.

Avoid Punitive Approaches

As noted previously, companies that suffer data breaches are victims of crimes. Without question, consumers and businesses that have their data stolen are victims of crime as well. Some media accounts of these incidents, however, seem to overlook what a significant and difficult problem it is to protect against data thieves. If the Defense Department and NSA can be hacked, it demonstrates how difficult the challenge is for private businesses to fully protect themselves. Given the difficulty, overly punitive measures are not appropriate in these situations. We are not saying that a failure to follow a notice law should not have any penalty associated with it. That can be necessary in some cases to get some businesses to comply. But the penalties should not be ones that are overwhelming, especially for small businesses. The goal should be to help businesses comply with the law to the greatest extent possible – not to play a "gotcha" game that leads to large fines. The costs of dealing with breaches, including paying forensic experts, lawyers, fraud costs, and dealing with reputational harms, already create strong economic incentives for businesses to try to avoid breaches. If one occurs, it should not simply be an excuse to pile on additional financial hits.

Pre-empt State Laws

As noted, there are two primary rationales for having a federal data breach law in light of the fact that the 51 state and territorial laws that currently exist cover the area well already. The first reason is to plug the holes that exist in the coverage of these laws today. Most prominently, a federal law would improve on the current set of data breach laws by removing the overly broad discretion given to financial institutions in the fourteen states that exempt them from their laws.

[9] 2013 Data Breach Investigations Report, Verizon.

The second reason for a federal law is to create a simpler and more efficient notice system. That way, businesses would only have to comply with one federal law rather than as many as 51 different ones. That efficiency can only be achieved if the state laws in this area are pre-empted. To the extent that pre-emption is not clear, a federal law would become the fifty-second law to comply with and the second rationale for having a federal law at all would be undermined. This pre-emption is necessary then for a federal law to make sense.

Pre-emption, however, makes it even more important to get any federal data breach law right. The state system currently ensures that people get notice in most of the situations that they should. That should not be undermined in the process of creating a federal law. In our view, the principles we've laid out above, if followed, would help protect against the potential negative consequences that could come from pre-emption. Given the hazards, however, we urge that the committee take its time and not rush through legislation before fully weighing all of the trade-offs between a federal bill and the state and territorial laws on the books.

Data Security

One thing worth emphasizing here is that data breach notification should not be the first priority in this area. As noted, notice is well-regulated today. Our first priority would be to focus on preventing data breaches. Merchants, including NACS and SIGMA members, collectively spend more than $6 billion per year just securing payment data.[10] Spending on all data security certainly exceeds this amount. Doing common-sense things like requiring PINs on payment card transactions, developing encryption and tokenization technologies that are effective (and open to all in the industry rather than creating competitive market problems), and increasing information-sharing with private industry and between the private sector and government are all measures that could demonstrably improve our ability to prevent data breaches in the first place. Many of the challenges in these areas stem from problematic standard-setting in the payment card arena and we would urge that particular attention be paid to those issues given the vulnerabilities that anti-competitive standard-setting has allowed to fester.

And, given the prevalence of foreign states in data breaches today, it may be time to more deeply examine to what extent our prism for viewing data security should be based on a national security model rather than a criminal justice model. It may be that, as with national security threats in the physical world, the resources available to data thieves are outstripping the ability of private businesses to individually deal with these threats. That is an issue that this and other committees ought to consider.

* * *

We appreciate the subcommittee providing us with this opportunity to submit our views on federal data breach legislation. We look forward to working with you as the committee continues to consider this topic.

[10] "Credit Card and Debit Card Fraud Statistics," CardHub 2013, available at http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/.